Review Of Prevention Techniques For Denial Of Service (DOS) Attacks In Wireless Sensor Network

Poonam Rolla, Manpreet Kaur

Abstract: Wireless Sensor Networks comprised of several tiny sensor nodes which are densely deployed over the region to monitor the environmental conditions. These sensor nodes have certain design issues out of which security is the main predominant factor as it effects the whole lifetime of network. DDoS (Distributed denial of service) attack floods unnecessary packets in the sensor network. A review on DDoS attacks and their prevention techniques have been done in this paper.

Keywords: DOS Attacks, Prevention techniques, Security Goal, Wireless sensor network.

I INTRODUCTION

A WSN is a wireless network consists of distributed sensor nodes used to monitor environmental conditions like temperature, sound etc. In WSN, DOS (Denial of service) attack makes weakness network. The packets travel repeatedly in the sensor network. By that all the resources like bandwidth, memory, energy are wasted by this attack. By avoiding these kinds of attacks network performance can be improved. The main aim of this paper is to review effect of various attacks in wireless sensor network and their prevention techniques. This paper includes introduction of Wireless Sensor Networks in Section 1, various attacks in Wireless Sensor Networks in Section 2, Defines the various DOS attacks in WSN in section 3 and prevention techniques proposed for DOS attacks are reviewed in section 4.Section 5 conclude the paper.

II. ATTACKS IN WSN

In WSN, there are micro sensor nodes in large area. These are of broadcast nature of the transitions medium so these need to be secure. Basically attacks are classified as active attacks and passive attacks.

A. Active Attacks

Malicious nodes damage other nodes due to network outage by partitioning; in this saving battery life is not a priority. Active attacks are:

1) HELLO Flood Attack

In wireless sensor network attacker sends HELLO packets from source node to destination node. Sensor nodes isolated in typical arranged area with in wireless sensor networks. So because of this problem sensor node does not identify that the enemy node is their neighbor. So as a result while sending the data to the sink the malicious node is trying to go through the attacker and they know that this malicious node is their neighbor and spoofed by the attacker.

- *Poonam Rolla, Department of CSE, Giani Zail Singh PTU Campus, Bathinda, India poonamrolla2@gmail.com*
- *Manpreet Kaur, Department of CSE, Giani Zail Singh PTU Campus, Bathinda, India sahez6548@gmail.com*

2) Denial of Service

A DOS attack (Denial of Service attack) is a type of attack that seeks to disrupt the function of the targeted computer network. DOS attack is the attack in which access amount of unnecessary packets flooded in network. Sensor nodes receive those packets and it also forwards those packets to its neighbors. Denial of service attack is multilayer attack [3]. In WSN there are many DOS attacks in different layers like jamming, tampering, collision and so on.

B. Passive Attacks

Selfish nodes use the network and do not cooperate with network, save battery life for their own communications; they do not directly damage other nodes.

III. DOS ATTACKS

In WSN, there are many ways to attempt DOS attack but we consider only two which are mainly effect the network. There are several types of Denial of service attack discuss as follows:

A. Denial of sleep attack

In Denial of sleep attack it targets the node's power consumption. In this attack attackers have knowledge of MAC layer protocol. The one protocol created for wireless sensor network is MAC protocol. When nodes are not sending and receiving data, the battery power of node stored by placing radio in low power modes. MAC protocol is available to overcome radio's primary sources of energy loss such as collision, control packet overhead and overhearing.

B. Path Based DOS attack

In path based DOS attack, attackers attacks on network. This is done by flooding the packets over multi hop end to end communication path. Path based DOS attack is easy to establish and it will destroy large portion of wireless sensor network [4]. In this node which process and summarize the data from member nodes, and send the result to a sink via a multihop, end-to end communication path and attackers create DOS in wireless sensor network by flood data packet along multi hop path which quickly affect the communication bandwidth, limited energy and memory [4].

C. Jamming attack

Jamming is the DOS attack which have two types such as Jamming under external threat model and internal threat

model [5]. In External model jammer is none of a part of network and jammer is randomly transmits high power interference signal. In internal model any attacker who knows network secretes and implementation details of protocol of the network product selective jamming attack.

D. Wormhole attack

In wormhole attack attacker record the every bit of packet or whole packet at one place. After recording the packet tunnel into the different location and then repeat them in to the network. This packet tunnel distance is longer than standard wireless transmission range of single hop. It is simple for attacker to make tunnel packet reach sooner as compare to other packets transmitted over a normal multi-hop route. Wormhole places the attacker in strong position to gain unauthorized access.

E. Vampire Attack

Vampire attacks not protocol-specific. It is the Denial of Service attack in which it consumes more energy, node can discharge and it can be disconnected from the network. Vampire attack is further divide in two different types of attacks which are Stretch attack and Carousel attack. These attacks are depends on reducing the energy of the nodes.

IV. DETECTION TECHNIQUES

A. Detection of Denial of Sleep attack

In denial of Sleep attack attacker have knowledge of MAC layer protocol and able to bypass encryption and authentication protocols.MAC layer protocol created for wireless sensor network and use different algorithm to store battery power by placing radio in low power mode. In this divide MAC protocol in four types i.e. Sensor MAC (SMAC), Berkeley MAC (B-MAC), Gateway MAC (GMAC) and Timeout MAC (T-MAC). Sensor-MAC frame divided to listening and Sleep period. The listening period divided into synchronization and transfer period. Periodic updating done by SYNC packet, Receivers will adjust their timer counters. All the nodes will announce their sleep schedule for correcting network time out in Sync period. TMAC is further an improvement in the S-MAC protocol by concentrating all traffic at the starting of the duty period .It shows transmitted and received messages. B-MAC does not attempt to sync sleep schedules. Berkeley-MAC uses the low-power listening (LPL) to reduce the energy consumption. G-MAC protocol used for improve network lifetime.

B. Detection of Path Based DOS attack

This DOS attack is establish by flooding packets along multi hop end to end network path. An intermediate node should able to detect spurious packet and have to reject them. To detect spurious packet and defend against path based DOS attack use secured lightweight mechanism. In this should be configures one way hash chain beside a path enabling each intermediate node for detecting a Path based DOS attack and prevents propagation of spurious packet. Every packet includes new one way hash chain number that is used for message authentication. Different hash chain number used for each time slot and intermediate node will forward packet only if new hash chain number will verified. This process of verification will continue and each time slot it verify new hash chain number. If number is not valid then drop the packet [4].

C. Detection of jamming attack

In jamming attack attacker attack in the network under external and internal threat model. Jammer is not part of the network in the external threat model. In external model jammer is sequentially forward high power interference signals [5]. To the defense from external jammer spreadspectrum communications technique used. Spread Spectrum techniques give bit-level protection by spreading bits according to a secret pseudo noise (PN) code known only to the communicating sensor nodes. In internal thread model any attacker who has knowledge of network protocol can establish selective jamming attack. To establish selective jamming attack attacker must be implement “classify then jam” earlier than culmination of forwarding task. Later than classification the attacker introduces a number of bit errors so that the packet cannot be recovered to the receiver. To prevent jamming attack from internal thread model, there is a method which is packet hiding method. In packet hiding method before classification of the packet by attacker hide the packets. Hence attacker can’t add bit error in the packet and it is securely forwarded. Methods for packet hiding are commitment methods and cryptographic puzzle. In first method sender commits the packet and it is verify by the verifier.

D. Detection of wormhole attack

For detection of wormhole attack we use Packet leash. There are two types of packet leash i.e. temporal and geographical. In temporal packet leash sender uses its timestamp .In geographical packet leash sender node uses its location and sending time of the packet to receiver .Based on this receiver estimates distance between sender node and receiver node. If the estimated distance is more as compare to the possible radio range then receiver will reject the communication.

E. Detection of Vampire attack

Vampire attack can be prevent using energy weight monitoring algorithm (EWMA).In this energy of the sensor node is consider for find out threshold level of the sensor node. To find out malicious node every node is add the test field when they will receive the packet and forward packet to other node and then test field is check for every node. If the test field is correct then normal operation will be continue and if the test field is not correct then creates an alarm packet and alarm packet is forwarded and announce that this node is malicious so that it avoid for communication. This algorithm is further divided in two phases that are communication phase and network configure phase. In network configuring phase create optimum routing path from source to destination. The node upon receiving this and stored it in routing table to facilitate computations. In communication phase it avoids same data packets forwarded repeatedly through same node. This copied packet compare with the data packet forwarding through the node. If the transmitted packet is matched with copied one then stop the packet transmitted. Thus it avoids the repeated packet transmitting through the same sensor node and protect from the vampire attack.

V. CONCLUSION

Wireless sensor network contains the number of tiny nodes, it forward the information from one node to another node continuously, That information are in the form of large packets, these packets flooded in the network and broadcast it to their neighbors. DoS attack can disrupt the entire network. Majority

of the DOS attacks can be overcome by authentication and anti-replay techniques. Other approaches are also available to detect DoS attack and get recovered from DOS attacks, these solutions can also be defeat by some counter techniques. That's why need to find out some concrete techniques and to do research work on them to get protected from DOS.

REFERENCES

[1] Chan, Haowen, and Adrian Perrig. "Security and privacy in sensor networks." Computer 36.10 (2003): 103-105.

[2] Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34.2 (2004): 39-53.

[3] Wood, Anthony D., and John A. Stankovic. "Denial of service in sensor networks." Computer 35.10 (2002): 54-62.

[4] Li, Bai, and Lynn Batten. "Using mobile agents to detect node compromise in path-based DoS attacks on wireless sensor networks." Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on. IEEE, 2007.

[5] Xu, Wenyuan, et al. "Jamming sensor networks: attack and defense strategies." Network, iEEE 20.3 (2006): 41-47.

[6] Jain, Sushil Kumar, and Kumkum Garg. "A hybrid model of defense techniques against base station jamming attack in wireless sensor networks." Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on. IEEE, 2009.

[7] Badal, Tapas, and Dipti Verma. "A Modular Approach for Intrusion Detection System in Wireless Networks." (2011): 57-61.

[8] Xie, Miao, et al. "Anomaly detection in wireless sensor networks: A survey." Journal of Network and Computer Applications 34.4 (2011): 1302-1325.

[9] M. Kaur, A. Jain and A. K. Goel, "Energy Efficient Two Level Distributed Clustering Scheme to Prolong Stability Period of Wireless Sensor Network", International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 68-73